

information necessary to reconstruct the reference table; and (3) a multiplexor multiplexes the compressed data and the encrypted data obtained from the encryptor to create multiplexed data that is output. Independent claims 12 and 14 are similar.

Independent claim 8 relates to a device for reproducing data by decompressing and decrypting multiplexed data, comprising, *inter alia*, a demultiplexor for extracting compressed data which is a compressed result obtained by compressing the original data and encrypted data which is an encrypted result obtained by encrypting a reference table to be referenced when performing data compression of the compressed data (to achieve compression of the original data), from input multiplexed data; a decoder for obtaining the reference table by decoding the encrypted data; and a decompressor for referencing the reference table to decompress the compressed data. Independent claims 13 and 15 are similar.

As set forth in Applicants' background, as data quantity increases, the amount of processing time expended to ensure safe encryption results in a significantly increased processing time or CPU load in proportion to the data size. Similar problems are faced by decryption. Thus, as discussed during the interview, the device of independent claim 1 achieves dramatically reduced processing time (see Applicants' page 10, lines 6-25) while ensuring security by (1) compressing original data and (2) encrypting the reference table or information necessary to reconstruct the reference table. Then, the compressed data (which does not require encryption) and the encrypted reference table data are multiplexed and output. Thus, regardless of the size of the original data, only a small reference table needs encryption in order to secure the data.

As admitted in the Office Action, Barbir merely achieves compression and encryption of the original data using a compression/encryption table (Col. 5, line 66), but fails to teach or suggest that the table itself (or information necessary to reconstruct the table) is encrypted.

Barbir also fails to teach or suggest multiplexing of compressed data and encrypted reference table information as recited in independent claims 1, 12 and 14.

As also admitted in the Office Action, Barbir fails to teach or suggest a demultiplexor for extracting compressed data and encrypted data which is an encrypted result obtained by encrypting a reference table to be referenced when performing data compression of the compressed data as recited in independent claim 8 and similarly fails to teach or suggest restoring a reference table to be referenced when carrying out data decompression by decoding the encrypted data as recited in independent claims 13 and 15.

For these noted deficiencies, the Office Action relies on Bledsoe. However, as discussed, the alleged passage on col. 4 is directed to Figure 1 and shows that original data from four different sources is multiplexed and that each source is encoded by a frequency code. That is, lookup tables in each encoder are used to control or limit the bits of the encoded original data to form output data, which is just a compressed version of the original data. Thus, as discussed, only the compressed original data from multiple sources is multiplexed. There is no teaching of encryption of the table or multiplexing of such encrypted reference table information with the compressed original data.

Instead, col. 7, lines 29-41 of Bledsoe indicate that the frequency table must be sent to the receiver. One of ordinary skill in the art would have considered this to be a separate unencrypted transmission as there is no mention of encryption or multiplexing with the compressed data. Clearly, Fig. 1 shows no encryption and multiplexing of table information.

Accordingly, even if combined, one of ordinary skill in the art would not have been led from such teachings to encrypt the reference table itself or information necessary to create the reference table or to multiplex this encrypted reference table information with the compressed original data as recited in independent claims 1, 12, and 14. One of ordinary skill in the art also would not have recognized an advantage or benefit to such features, such as a

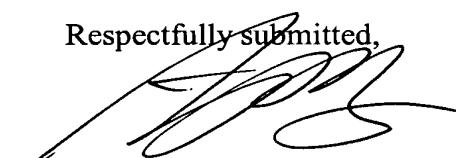
secure encryption with limited processing regardless of the file size. Additionally, because received data does not include multiplexed data comprising compressed original data and encrypted reference table information, one of ordinary skill in the art would not have been led from such teachings to provide a demultiplexing step or a demultiplexor as recited in independent claims 8, 13, and 15.

Thus, because Bledsoe fails to overcome the deficiencies of Barbir with respect to each of independent claims 1, 8, and 12-15, these claims and claims dependent therefrom are not obvious. Withdrawal of the rejection is respectfully requested.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-15 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Stephen P. Catlin
Registration No. 36,101

JAO:SPC/axl

Date: October 11, 2007

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461
--